

**BROADCASTING AND RECEIVING SYSTEM AND ASSOCIATED  
CONDITIONAL ACCESS SYSTEM****Publication number:** RU2196389 (C2)**Publication date:** 2003-01-10**Inventor(s):** BAJASI MULKHAM [FR]; DE LA TJULE P ER [FR]; ZHEZEKEL  
ZHAN-FRANSUA [FR]**Applicant(s):** KANAL & SOS ETEH ANONIM [FR]**Classification:**

**- international:** G06F9/445; G06F9/06; G06F9/46; G06F11/00; G06F11/08;  
G06F11/10; G06F11/26; G06F11/28; G06F12/00; G06F12/02;  
G06F13/00; G06F13/10; G06F21/24; G06K17/00; G06K19/00;  
G06K19/07; G06T9/00; G09C1/00; G11C8/06; G11C16/02;  
H04B1/713; H04H20/02; H04H40/00; H04L1/00; H04L9/10;  
H04L9/32; H04L12/56; H04L13/08; H04L29/10; H04N5/00;  
H04N5/222; H04N5/44; H04N5/455; H04N7/14; H04N7/16;  
H04N7/167; H04N7/173; H04N7/24; H04N7/26; H04N7/66;  
H04N17/00; H04N17/04; G06F9/445; G06F9/06; G06F9/46;  
G06F11/00; G06F11/08; G06F11/10; G06F11/26; G06F11/28;  
G06F12/00; G06F12/02; G06F13/00; G06F13/10; G06F21/00;  
G06K17/00; G06K19/00; G06K19/07; G06T9/00; G09C1/00;  
G11C8/00; G11C16/02; H04B1/69; H04H1/00; H04H1/04;  
H04H9/00; H04L1/00; H04L9/10; H04L9/32; H04L12/56;  
H04L13/08; H04L29/10; H04N; H04N5/00; H04N5/222;  
H04N5/44; H04N5/455; H04N7/14; H04N7/16; H04N7/167;  
H04N7/173; H04N7/24; H04N7/26; H04N7/64; H04N17/00;  
H04N17/04; (IPC1-7): H04H9/00; H04N5/222

**- European:** H04N7/173B; G06T9/00T

**Application number:** RU19990121864 19970425**Priority number(s):** EP19970400650 19970321**Also published as:**

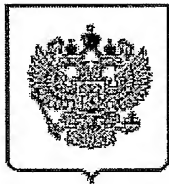
RU2226746 (C2)

**Abstract of RU 2196389 (C2)**

FIELD: satellite digital television systems. SUBSTANCE: satellite digital television system has plurality of computer attachments (STB) corresponding to plurality of end user television sets, modem and decoder arranged in each STB, subscriber authorizing system (SAS) incorporating or coupled with plurality of communication servers, facilities included in SAS for generating entitlement management messages (EMM), return channel connecting separate STBs with SASs, facilities included in SAS and in each STB so that desired information for entering respective EMM in system is submitted directly to respective communication server incorporated in SAS or coupled with the latter to authorize mentioned EMM transmission, and/or facilities for connecting modem to return channel,; and facilities enabling EMM transmission to decoder directly from respective server incorporated in SAS or coupled with the latter. Some other important features are also described. EFFECT: reduced delay time in transmitting entitlement management messages. 25 cl, 20 dwg

---

Data supplied from the esp@cenet database — Worldwide

(19) **RU** (11) **2196389** (13) **C2**

(51) 7 H04H9/00, H04N5/222

ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,  
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

**(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Статус: по данным на 11.01.2009 - действует

- (21) Заявка: 99121864/09  
 (22) Дата подачи заявки: 1997.04.25  
 (24) Дата начала отсчета срока действия патента: 1997.04.25  
 (31) Номер конвенционной заявки: 97400650.4  
 (32) Дата подачи конвенционной заявки: 1997.03.21  
 (33) Страна приоритета: EP  
 (45) Опубликовано: 2003.01.10  
 (56) Список документов, цитированных в отчете о поиске: US 5144663 A, 01.09.1992. WO 94/14284 A1, 23.06.1994. RU 95108701 A1, 10.02.1997. US 5195134 A, 16.03.1993. US 5206906 A, 27.05.1993.  
 (71) Заявитель(и): КАНАЛЬ+ СОСЬЕТЭ АНОНИМ (FR)  
 (72) Автор(ы): БАЙАСИ Мулхам (FR); ДЕ ЛА ТЮЛЕ Пьер (FR); ЖЕЗЕКЕЛЬ Жан-Франсуа (FR)  
 (73) Патентообладатель(и): КАНАЛЬ+ СОСЬЕТЭ АНОНИМ (FR)  
 (74) Патентный поверенный: Поликарпов Александр Викторович  
 (85) Дата соответствия ст.22/39 РСТ: 1999.10.21  
 (86) Номер и дата международной или региональной заявки: EP 97/02108 (25.04.1997)  
 (87) Номер и дата международной или региональной публикации: WO 98/43426 (01.10.1998)  
 Адрес для переписки: 193036, Санкт-Петербург, а/я 24, "НЕВИНПАТ", пат.пов. А.В.Поликарпову

**(54) СИСТЕМА ВЕЩАНИЯ И ПРИЕМА, А ТАКЖЕ СИСТЕМА УСЛОВНОГО ДОСТУПА ДЛЯ НЕЕ**

Изобретение относится к системе вещания и приема и системе условного доступа для нее. Техническим результатом является уменьшение времени задержки при передаче сообщений управления предоставлением прав. Это достигается тем, что система цифрового спутникового телевидения включает множество компьютерных приставок (STB), соответствующих множеству телевизионных приемников конечных пользователей, модем и декодер, располагающийся в каждом STB, систему санкционирования подписчиков (SAS), содержащую или связанную с множеством серверов связи, средства, включенные в SAS, для генерирования сообщений управления предоставлением прав (EMM), обратный канал, соединяющий отдельно каждую STB с SAS, средства, включенные в SAS и каждый STB, так что необходимая информация, требуемая для ввода соответствующего EMM в систему, предоставляется непосредственно в соответствующий сервер связи, включенный в SAS или связанный с ней, для санкционирования отправления упомянутого EMM, и/или средства для подключения модема к обратному каналу и средства, с помощью которых EMM передается в декодер непосредственно из соответствующего сервера связи, входящего в SAS или связанного с ней. Описываются также другие важные особенности. 6 с. и 19 з.п.ф-лы, 20 ил.

**ОПИСАНИЕ ИЗОБРЕТЕНИЯ**

Предлагаемое изобретение относится к системе вещания и приема, в частности к цифровой интерактивной системе спутникового телевидения, ориентированной на массовый рынок, и системе условного доступа для нее.

В частности, но не исключительно, изобретение относится к системам вещания для массового потребителя, имеющим некоторые или все следующие предпочтительные особенности:

- это информационная система вещания, предпочтительно система радио и/или телевизионного вещания;
- это спутниковая система (хотя она может быть использована для кабельной или наземной трансляции);
- это цифровая система, предпочтительно использующая систему сжатия MPEG, более предпочтительно MPEG-2, для трансляции данных/сигналов;
- она допускает возможность интерактивной работы.

Более конкретно, предлагаемое изобретение относится к так называемому платному телевидению (или радио), в котором пользователь/зритель выбирает программу/фильм/игру для просмотра, которая должна быть оплачена, что называется уплатой за просмотр (PPV - Pay Per View, уплата производится за каждую просмотренную передачу) или, в случае загрузки данных, оплатой за файл, или пофайловой оплатой (PPF).

В таких известных PPV и PPF системах пользователь/зритель должен затратить значительное количество времени на выполнение действий, необходимых для фактического доступа к выбранному продукту.

Например, в одной известной системе должна быть выполнена следующая последовательность шагов:

- i) Пользователь звонит в так называемую систему управления подписчиками (SMS), которая в этой известной системе включает несколько людей-операторов, которые отвечают на звонок подписчика, и которой подписчик сообщает необходимую информацию, касающуюся выбранного продукта и касающуюся финансового состояния подписчика для так называемой системы санкционирования подписчиков (SAS), которая включает в себя или связана с множеством серверов связи.
- ii) Затем оператор в SMS должен проверить финансовое состояние пользователя, прежде чем санкционировать связь между серверами связи и телевизором пользователя, чтобы продукт мог быть отправлен и затем просмотрен пользователем.

В другой известной системе человек-оператор заменяется автоматическим голосовым сервером, так что когда пользователь звонит в SMS он/она слышит активируемую голосом запись, на которую пользователь сообщает ту же информацию, что и в пункте i) выше.

В указанной второй системе уменьшается задержка, которая имеет место в первой из описанных систем, которая более подвержена перегрузке в случаях, когда большое количество пользователей желают заказать продукт одновременно.

Тем не менее, даже во второй системе пользователю приходится вводить значительный объем информации в виде длинной последовательности цифр, и эта операция может приводить к большому числу ошибок и занимает много времени.

Третья известная система предполагает использование пользователем известных экранных систем, такой как MINITEL во Франции или PRESTEL в Великобритании, которая заменяет активируемый голосом сервер, упомянутый выше в описании второй системы. Сами системы MINITEL и PRESTEL используют со стороны клиента модем.

Во всех этих известных системах пользователь вынужден затратить много времени и усилий при вводе всей той информации, которая необходима системе для разрешения санкционирования передачи выбранного продукта в телевизор пользователя.

В случае системы спутникового телевидения возникает дополнительная задержка фактического приема пользователем выбранного продукта.

В PPV и PPF системах ключевыми элементами управления доступом пользователей к продуктам являются так называемые сообщения управления предоставлением прав (EMM - Entitlement Management Messages), которые должны быть введены в систему для того, чтобы предоставить

пользователю доступ к продукту. Более конкретно, ЕММ являются тем механизмом, с помощью которого зашифрованные данные, представляющие продукт, расшифровываются для конкретного индивидуального пользователя.

В известных системах спутникового телевидения ЕММ передаются в телевизоры пользователей по спутниковому каналу в потоке данных MPEG-2 через регулярные интервалы времени. Следовательно, для ЕММ конкретного пользователя может возникать значительная задержка длительностью в несколько минут до того, как переданный следующий ЕММ пользователя поступит в телевизор данного пользователя.

Эта задержка передачи добавляется к упомянутой выше задержке, возникающей вследствие того, пользователь вынужден вводить данные в систему вручную. Эффект накопления этих задержек приводит к тому, что для получения доступа к выбранному продукту пользователю может потребоваться потратить, например, пять минут.

Настоящее изобретение предназначено для преодоления этой проблемы.

Согласно первому аспекту данного изобретения предлагается система условного доступа, содержащая:

средства генерирования множества сообщений (предпочтительно условного доступа); и

средства для приема сообщений, выполненные с возможностью осуществления связи с упомянутыми средствами генерирования через сервер связи, подключенный непосредственно к упомянутым средствам генерирования.

Предпочтительно это сообщение является сообщением о правах для передачи (например, путем вещания) на средства приема, причем упомянутые средства генерирования выполнены с возможностью генерирования сообщений о правах в ответ на данные, принимаемые от упомянутых средств приема.

Средства генерирования могут быть выполнены с возможностью передачи сообщения как пакета цифровых данных на упомянутые средства приема либо через упомянутый сервер связи, либо через спутниковый ретранслятор.

Средства приема могут быть подключены к упомянутому серверу связи через модем или канал.

В соответствии с альтернативным вариантом, настоящее изобретение предлагает систему условного доступа для обеспечения условного доступа для подписчиков, содержащую:

систему управления подписчиками;

систему санкционирования подписчиков, подключенную к системе управления подписчиками; и

сервер связи, который подключается непосредственно к системе санкционирования подписчиков.

Система может дополнительно содержать приемник/декодер для подписчика, этот приемник/декодер может быть подключен к упомянутому серверу и, следовательно, к упомянутой системе санкционирования подписчиков, через модем и телефонный канал.

Согласно второму аспекту настоящего изобретения предлагается система вещания и приема, включающая систему условного доступа, описанную выше.

В третьем аспекте предлагаемое изобретение предоставляет систему вещания и приема, содержащую:

средства генерирования множества сообщений о правах, относящихся к вещаемым программам;

средства для приема упомянутых сообщений от упомянутых средств генерирования; и

средства связи средств приема со средствами генерирования для выполнения приема упомянутых

сообщений, упомянутые средства связи могут осуществлять специализированную связь между средствами приема и средствами генерирования.

Специализированная связь обычно представляет собой проводное соединение и/или связь через модем с возможностью связи через сотовую телефонную систему. Другими словами, специализированная связь предоставляет канал передачи информации (от точки к точке), в противоположность вещанию информации через эфир или окружающей среде. Средства связи в средствах приема обычно представляют собой модем.

Следовательно, в существенно подобном варианте, настоящим изобретением предлагается система вещания и приема, содержащая:

средства генерирования множества сообщений о правах, относящихся к вещаемым программам;

средства для приема через модем упомянутых сообщений от упомянутых средств генерирования; и

средства для соединения упомянутого модема с упомянутыми средствами генерирования и упомянутыми средствами приема.

Приведенные выше особенности обеспечивают возможность предоставления пользователю необходимых прав просмотра (с помощью EMM) быстрее, чем было возможно ранее, частично потому, что, поскольку SAS обычно реализуется меньшим количеством программного кода, чем SMS, SAS может работать более эффективно (и в реальном времени), частично потому, что SAS может сама непосредственно генерировать необходимое EMM, и частично потому, что EMM может передаваться пользователю или подписчику по специализированному (обычно модемному) каналу.

Предпочтительно средства генерирования подключаются к упомянутому модему через сервер связи, который предпочтительно входит в состав или связан с упомянутыми средствами генерирования.

Средства приема могут быть также выполнены с возможностью приема упомянутых сообщений о правах через спутниковый ретранслятор.

Средствами приема может быть приемник/декодер, содержащий средства для приема сжатых сигналов MPEG-типа, средства декодирования принятых сигналов для получения телевизионного сигнала и средства передачи телевизионного сигнала в телевизор.

Предпочтительно средства приема выполнены с возможностью связи с упомянутыми средствами генерирования через упомянутый модем и средства связи. Средства приема могут содержать средства чтения смарт-карты, вставляемой конечным пользователем, которая содержит сохраненные данные для автоматического инициирования передачи сообщения от упомянутых средств приема в упомянутые средства генерирования после установки смарт-карты конечным пользователем.

Кроме этого, система может дополнительно содержать голосовой канал для обеспечения связи со средствами генерирования конечному пользователю системы вещания и приема.

Как следует из приведенного выше, настоящее изобретение предлагает два усовершенствования, с помощью которых уменьшается время, требуемое конечному пользователю для доступа к желаемому продукту. Предпочтительно, чтобы для достижения максимальной экономии времени использовались оба усовершенствования, однако возможно отдельное использование каждого из них.

Согласно следующему аспекту настоящего изобретения, предлагается система вещания и приема, содержащая со стороны вещания:

систему вещания, включающую в себя средства для вещания запроса обратного вызова;

и со стороны приема:

приемник, включающий в себя средства для обратного вызова системы вещания в ответ на запрос обратного вызова.

Путем обеспечения того, что система вещания может запросить обратный вызов от приемника, системе вещания обеспечивается возможность получения информации от приемника о состоянии

приемника.

Предпочтительно средства для осуществления обратного вызова системы вещания содержат модем, подключаемый к телефонной системе. Использование обратного модемного канала предоставляет простой путь реализации изобретения на практике.

Также предпочтительно средства для осуществления обратного вызова системы вещания с возможностью передачи в систему вещания информации о приемнике. Это информация может содержать количество оставшихся жетонов, количество предварительно заказанных сеансов и т.д.

Предпочтительно система вещания содержит средства для хранения упомянутой информации с целью ее последующей обработки в случае необходимости.

Предпочтительно средства вещания выполнены с возможностью вещания запроса обратного который включает в себя команду, согласно которой обратный вызов выполняется в заданное время, и средства для осуществления обратного вызова системы вещания выполнены с возможностью ответа на упомянутую команду. Путем обеспечения обратного вызова после фактического получения запроса обеспечивается дополнительная гибкость системы.

Средства вещания могут быть выполнены с возможностью вещания в качестве запроса обратного вызова одного или нескольких сообщений о правах.

Предпочтительно система вещания включает средства для генерирования контрольного сообщения (например, случайного числа) и передачи его в приемник, приемник содержит средства для шифровки контрольного сообщения и передачи его в систему вещания, и система вещания дополнительно содержит средства для дешифровки контрольного сообщения, принимаемого от приемника, и сравнения его с оригинальным контрольным сообщением. Таким образом можно проверить, является ли приемник действительным и оригинальным.

Любые из перечисленных выше особенностей могут быть объединены в любое необходимое сочетание. Они могут также предоставляться, при необходимости, в вариантах способа.

Предпочтительные особенности данного изобретения будут сейчас описаны, путем описания одного из примеров, со ссылками на прилагаемые чертежи, среди которых:

на фиг. 1 изображена общая архитектура системы цифрового телевидения, соответствующая предпочтительному варианту реализации данного изобретения;

на фиг. 2 - архитектура системы условного доступа системы цифрового телевидения;

на фиг.3 - структура EMM, используемого в системе условного доступа;

на фиг. 4 - принципиальная схема аппаратного обеспечения системы санкционирования подписчиков (SAS) в соответствии с предпочтительной реализацией данного изобретения;

на фиг.5 - принципиальная схема архитектуры SAS;

на фиг. 6 - принципиальная схема сервера технического управления подписчиками, являющегося частью SAS;

на фиг.7 - блок-схема процедуры автоматического восстановления подписок, реализуемая SAS;

на фиг. 8 - принципиальная схема битового массива подписки группы, используемого в процедуре автоматического восстановления;

на фиг.9 - структура EMM, используемого в процедуре автоматического восстановления;

на фиг.10 - подробная структура EMM;

на фиг.11 - принципиальная схема централизованного сервера заказов, при его использовании для приема команд непосредственно через серверы связи;

на фиг.12 - диаграмма, иллюстрирующая часть фиг. 2, где показан один из вариантов реализации

данного изобретения;

на фиг.13 - принципиальная схема централизованного сервера заказов, при его использовании для приема команд от системы санкционирования подписчиков, для запроса обратного вызова;

на фиг.14 - принципиальная схема серверов связи;

на фиг. 15 - варьирование частоты повторения передачи EMM в зависимости от времени трансляции PPV-программы;

на фиг.16 - принципиальная схема передатчика сообщений для генерирования EMM;

на фиг. 17 - принципиальная схема, иллюстрирующая способ хранения EMM в передатчике сообщений;

на фиг.18 - принципиальная схема смарт-карты;

на фиг.19 - схема размещения разделов в памяти смарт-карты;

на фиг.20 - схематическая диаграмма описания PPV-программы.

Общая структура системы вещания и приема цифрового телевидения 1000 согласно данному изобретению приведена на фиг. 1. Изобретение включает практически обычную систему цифрового телевидения 2000, которая использует известную систему сжатия MPEG-2 для передачи сжатых цифровых сигналов. Более подробно, устройство сжатия MPEG-2 2002 в центре вещания принимает поток цифровых сигналов (обычно поток видеосигналов). Устройство сжатия 2002 подключается к мультиплексору и скремблеру 2004 с помощью канала 2006. Мультиплексор 2004 принимает множество входных сигналов, собирает один или несколько несущих потоков и передает сжатые цифровые сигналы в передатчик 2008 центра вещания через канал 2010, тип которого, естественно, может быть различным, включая каналы телекоммуникаций. Передатчик 2008 передает электромагнитные сигналы через канал "земля-спутник" 2012 на спутниковый ретранслятор 2014, где выполняется их обработка электронными средствами и вещание через виртуальный канал "спутник-земля" 2016 на наземный приемник 2018, обычно имеющий форму тарелки, принадлежащий конечному пользователю или арендуемый им. Сигналы, принимаемые приемником 2018, передаются в совмещенный приемник/декодер 2020, принадлежащий конечному пользователю или арендуемый им, и подключенный к телевизору 2022 конечного пользователя. Приемник/декодер 2020 декодирует сжатый MPEG-2 сигнал в телевизионный сигнал для телевизора 2022.

Система условного доступа 3000 подключается к мультиплексору 2004 и приемнику/декодеру 2020 и располагается частично в центре вещания и частично в декодере. Она позволяет конечному пользователю осуществлять доступ к вещательным передачам цифрового телевидения от одного или нескольких операторов вещания. В приемник/декодер 2020 может устанавливаться смарт-карта, которая может декодировать сообщения, относящиеся к коммерческим предложениям (одна или несколько телевизионных программ, продаваемых оператором вещания). С использованием декодера и смарт-карты пользователь может покупать передачи в режиме подписки или оплаты за просмотр (PPV).

Интерактивная система 4000, также подключенная к мультиплексору 2004 и приемнику/декодеру и также располагающаяся частично в центре вещания и частично в декодере, позволяет конечному пользователю взаимодействовать с различными приложениями через модемный обратный канал 4002.

Далее будет описана более подробно система условного доступа 3000.

Как показано на фиг.2, говоря в общем, система условного доступа 3000 включает систему санкционирования подписчиков (SAS) 3002. SAS 3002 подключена к одной или более системам управления подписчиками (SMS) 3004, по одной SMS для каждого оператора вещания, посредством соответствующего канала TCP-IP 3006 (хотя в альтернативных реализациях вместо него могут использоваться каналы других типов). В альтернативном варианте одна или несколько SMS могут использоваться совместно двумя операторами вещания, либо один оператор может использовать две SMS и т.д.

Первые устройства шифрования в виде шифровальных блоков 3008, использующих "материнские" смарт-карты 3010, подключаются к SAS через канал связи 3012. Вторые устройства шифрования,

также в виде шифровальных блоков 3014, использующих материнские смарт-карты 3016, подключаются к мультиплексору 2004 через канал связи 3018. Приемник/декодер 2020 принимает "дочернюю" смарт-карту 3020. Он подключается непосредственно к SAS 3002 с помощью серверов связи 3022 через модемный обратный канал 4002. SAS, наряду с другими сигналами, по запросу посылает в дочернюю карту права подписки.

Смарт-карты содержат "секреты" одного или нескольких коммерческих операторов. "Материнская" смарт-карта шифрует различные виды сообщений, а "дочерние" смарт-карты расшифровывают эти сообщения, если у них есть на это права.

Первый и второй шифровальные блоки 3008 и 3014 содержат шасси, электронную плату VME, программное обеспечение которой записано в электрически-стираемом программируемом ПЗУ, до 20 электронных плат и одну смарт-карту 3010 и 3016 соответственно для каждой электронной платы, одну (карта 3016) для шифровки ECM и одну (карта 3010) для шифровки EMM.

Далее будет описана более подробно работа системы условного доступа 3000 системы цифрового телевидения относительно различных компонентов системы телевидения 2000 и системы условного доступа 3000.

#### Мультиплексор и скремблер

На фиг.1 и 2 показано, что в центре вещания цифровой видеосигнал сначала сжимается (или скорость передачи уменьшается) с использованием устройства сжатия MPEG-2 2002. Этот сжатый сигнал затем передается в мультиплексор и скремблер 2004 через канал связи 2006 для того, чтобы мультиплексировать его с другими данными, такими как другие сжатые данные.

Скремблер генерирует слово управления, используемое в процессе скремблирования и включаемое в поток данных MPEG-2 в мультиплексоре 2004. Слово управления генерируется внутри системы и позволяет совмещенному приемнику/декодеру конечного пользователя 2020 дескремблировать программу.

В поток данных MPEG-2 добавляются также критерии доступа, указывающие, каким образом программа предлагается потребителям. Программа может предлагаться как в одном из многих режимов "подписки", так и/или в одном из многих режимов "с оплатой за просмотр" (PPV). В режиме подписки конечный пользователь подписывается на одно или несколько коммерческих предложений, или "букеты", получая, таким образом, права на просмотр любого канала из этих букетов. В предпочтительном варианте реализации из букета каналов можно выбрать до 960 коммерческих предложений. В режиме оплаты "за просмотр" конечному пользователю предоставляется возможность покупать передачи по желанию. Это может обеспечиваться путем предварительного заказа передач ("режим предварительного заказа") или путем приобретения программы сразу после начала вещания ("импульсный режим"). В предпочтительной реализации все пользователи являются подписчиками независимо от режима просмотра - подписка или PPV, но, конечно, PPV-зрители не обязательно должны быть подписчиками.

Как слово управления, так и критерии доступа используются для формирования сообщения управления правами (ECM); указанное сообщение является сообщением, подлежащим отсылке вместе с одной скремблированной программой; сообщение содержит слово управления (которое позволяет дескремблировать программу) и критерии доступа вещательной программы. Критерии доступа и слово управления передаются на второй шифровальный блок 3014 через канал связи 3018. В этом блоке ECM генерируется, зашифровывается и передается в мультиплексор и скремблер 2004.

Каждая услуга, вещаемая оператором вещания в потоке данных, содержит несколько различных компонент; например, телевизионная программа включает видеокomпоненту, аудиокomпоненту, компоненту субтитров и т.д. Каждая из этих компонент услуги для последующего вещания на ретранслятор 2014 скремблируется и зашифровывается отдельно. Для каждой скремблированной компоненты услуги требуется отдельное ECM.

#### Трансляция программы

Мультиплексор 2004 принимает электрические сигналы, содержащие зашифрованные EMM, от SAS 3002, зашифрованные ECM от второго шифровального блока 3014 и сжатые программы от устройства сжатия 2002. Мультиплексор 2004 скремблирует программы и передает скремблированные программы, скремблированные EMM и скремблированные ECM в виде



электрических сигналов на передатчик 2008 центра вещания через канал связи 2010. Передатчик 2008 передает электромагнитные сигналы на спутниковый ретранслятор 2014 через канал "земля-спутник" 2012.

#### Прием программ

Спутниковый ретранслятор 2014 принимает и обрабатывает электромагнитные сигналы, передаваемые передатчиком 2008, и передает эти сигналы на наземный приемник 2018, обычно имеющий форму тарелки, принадлежащий конечному пользователю или арендуемый им, через канал "спутник-земля". Сигналы, принимаемые приемником 2018, передаются в совмещенный приемник/декодер 2020, принадлежащий конечному пользователю или арендуемый им, и подключенный к телевизору конечного пользователя 2022. Приемник/декодер 2020 демультимплексирует сигналы с целью получения скремблированных программ с зашифрованными EMM и зашифрованными ECM.

Если программа не скремблированная, т.е. с потоком данных MPEG-2 ECM не передается, приемник/декодер 2020 выполняет декомпрессию данных и преобразует сигнал в видеосигнал для передачи его в телевизор 2022.

Если программа скремблированная, приемник/декодер 2020 извлекает из потока данных MPEG-2 соответствующее ECM и передает ECM в "дочернюю" смарт-карту 3020 конечного пользователя. Она вставляется в гнездо приемника/декодера 2020. Дочерняя смарт-карта 3020 контролирует, имеет ли пользователь права на дешифровку данного ECM и на доступ к данной программе. Если нет, то в приемник/декодер 2020 передается отрицательный результат, указывающий, что программа не может быть дескремблирована. Если конечный пользователь имеет такие права, ECM расшифровывается и извлекается слово управления. Декодер 2020 может затем дескремблировать программу с использованием данного слова управления. Затем выполняется декомпрессия потока данных MPEG-2 и его преобразование в видеосигнал для дальнейшей передачи в телевизор 2022.

#### Система управления подписчиками (SMS)

Система управления подписчиками (SMS) 3004 содержит базу данных 3024, которая управляет, помимо прочего, всеми файлами конечных пользователей, коммерческими предложениями (такими как тарифы и поощрения), подписками, информацией, относящейся к PPV, и данными, касающимися потребления и санкционирования конечного пользователя. SMS может быть физически удалена от SAS.

Каждая SMS 3004 передает в SAS 3002 через соответствующий канал связи 3006 сообщения, которые вызывают преобразование или создание сообщений управления предоставлением прав (EMM), подлежащих передаче конечному пользователю.

SMS 3004 также передает в SAS 3002 сообщения, которые не предполагают какого бы то ни было преобразования или создания сообщений EMM, но предполагает только изменение состояния конечного пользователя (относительно санкционирования, предоставляемого конечному пользователю при заказе продукта, или суммы, на которую конечный пользователь будет дебитован).

Как будет описано ниже, SAS 3002 посылает сообщения (обычно запрашивающие информацию, такую как информация обратного запроса или информация о счете) в SMS 3004, так что очевидно, что связь между этими двумя системами является двухсторонней.

#### Сообщения управления предоставлением прав (EMM)

EMM - это сообщение, предназначенное для индивидуального конечного пользователя (подписчика) или группы конечных пользователей (в противоположность ECM, которое предназначается лишь для одной скремблированной программы или набора скремблированных программ, представляющих часть одного коммерческого предложения). Каждая группа может содержать заданное количество конечных пользователей. Такая организация в виде группы имеет целью оптимизировать использование полосы пропускания; таким образом, доступ к одной группе может позволить достичь большого числа конечных пользователей.

Для практической реализации данного изобретения используются различные специальные типы EMM. Индивидуальные EMM предназначены для индивидуальных подписчиков и обычно используются при предоставлении PPV-услуг; они содержат идентификатор группы и позицию

подписчика в этой группе. Так называемые EMM "групповой" подписки предназначены для групп из, положим, 256 индивидуальных пользователей, и используются обычно для администрирования некоторых услуг по подписке. Такое EMM содержит идентификатор группы и битовый массив подписчиков группы. Зрительские EMM предназначены для всей зрительской аудитории и могут, например, использоваться операторами для предоставления некоторых бесплатных услуг. "Зрители" - это вся совокупность подписчиков, имеющих смарт-карты с одинаковыми идентификаторами оператора (OPI - Operator Identifier). И, наконец, "уникальные" EMM адресованы для уникальных идентификаторов смарт-карт.

Структура типового EMM представлена на фиг.3. В общем, EMM, которое реализуется в виде последовательности битов цифровых данных, состоит из заголовка 3060, собственно EMM 3062 и подписи 3064. Заголовок 3060, в свою очередь, состоит из идентификатора типа 3066 для идентификации типа EMM -индивидуальный, групповой, зрительский или какой-либо другой, идентификатора размера 3068, который указывает размер EMM, необязательного адреса 3070 для EMM, идентификатора оператора 3072 и идентификатора ключа 3074. Собственно EMM, естественно, существенно различается в зависимости от его типа. И, наконец, подпись 3064, которая обычно имеет размер 8 байтов, содержит информацию для борьбы с искажениями остальных данных в EMM.

#### Система санкционирования подписчиков (SAS)

Сообщения, генерируемые SMS 3004, передаются через канал связи 3006 в систему санкционирования подписчиков (SAS) 3002, которая, в свою очередь, генерирует сообщения, подтверждающие прием сообщений, генерируемых SMS 3004, и передает эти подтверждения в SMS 3004.

Как показано на фиг.4, на уровне аппаратных средств SAS известным образом состоит из мэйнфрейм-компьютера 3050 (в предпочтительном варианте реализации - компьютера DEC), связанного с одной или несколькими клавиатурами 3052 для ввода данных и команд, одним или несколькими видеомониторами (VDU - Visual Display Unit) 3054 для отображения выходной информации и средствами хранения данных 3056. Может иметь место некоторая избыточность аппаратных средств.

На уровне программного обеспечения в предпочтительном варианте реализации SAS под управлением стандартной открытой операционной системы VMS выполняет комплекс программных средств, архитектура которых будет описана ниже в общем виде со ссылкой на фиг. 5; очевидно, что программные средства могут быть, как альтернатива, реализованы аппаратно.

В общем виде, SAS содержит область ветви подписки 3100 для предоставления прав в режиме подписки и для ежемесячного автоматического восстановления прав, область ветви PPV (оплаты за просмотр) 3200 для предоставления прав для PPV-передач, и инжектор EMM 3300 для передачи сообщений EMM, создаваемых в областях ветвей подписки и PPV, в мультиплексор и скремблер 2004 с последующей их подачей в поток данных MPEG. Если должны быть предоставлены другие права, такие как права пофайловой оплаты (PPF - Pay Per File) в случае загрузки компьютерного программного обеспечения в персональный компьютер пользователя, предусматриваются также другие подобные области.

Одна из функций SAS 3002 состоит в управлении правами доступа к телевизионным программам, доступным как коммерческие предложения в режиме подписки или продаваемым в режиме PPV-передач в соответствии с различными коммерческими режимами (режим предварительного заказа, импульсный режим). SAS 3002, в соответствии с правами и информацией, принимаемыми от SMS 3004, генерирует для подписчика сообщения EMM.

Область ветви подписки 3100 включает интерфейс команд (CI - Command Interface) 3102, сервер технического управления подписчиками (STM - Subscriber Technical Management) 3104, генератор сообщения (MG - Message Generator) 3106 и шифровальный блок (CU - CIPHERING Unit) 3008.

Область ветви PPV 3200 содержит сервер санкционирования (AS -Authorisation Server) 3202, реляционную базу данных 3204 для хранения необходимой информации о конечных пользователях, база данных локального черного списка 3205, серверы баз данных 3206 для указанной базы данных, централизованный сервер заказов (OCS - Order Centralised Server) 3207, сервер для вещательных компаний (SPB) 3208, генератор сообщения (MG) 3210, функции которого в основном те же, что и генератора сообщений области ветви подписки, и поэтому далее подробно не описываются, и шифровальный блок 3008.

Инжектор EMM 3300 состоит из множества источников сообщений (ME - Message Emitters) 3302, 3306 и 3308 и программных мультиплексоров (SMUX - Software MultipleXer) 3310 и 3312. В предпочтительном варианте реализации имеются два ME, 3302 и 3304, для генератора сообщений (MG) 3106, и два других ME, 3306 и 3308, для генератора сообщений (MG) 3210. ME 3302 и 3306 подключаются к SMUX 3310, а ME 3304 и 3308 подключаются к SMUX 3312.

Каждый из трех главных компонентов SAS (область ветви подписки, область ветви PPV и инжектор EMM) ниже будет рассмотрен более детально.

#### Область ветви подписки

Рассмотрим сначала область ветви подписки 3100, в которой интерфейс команд CI 3102 предназначен в первую очередь для отправки сообщений из SMS 3004 в сервер STM 3104, а также в OCS 3206, и из OCS в SMS. Интерфейс команд принимает от SMS в качестве входных данных как непосредственные команды, так и пакетные файлы, содержащие команды. Он выполняет синтаксический анализ сообщений, поступающих от сервера STM, и может формировать точные сообщения, если в принимаемом сообщении содержится ошибка (параметр вне пределов диапазона, параметр пропущен и т.д.). Он протоколирует поступающие команды в текстовой форме в файле трассировки 3110 и в двоичной форме в файле воспроизведения 3112 для того, чтобы иметь возможность воспроизвести последовательности команд. Протоколирование может быть отключено и размер файла ограничен.

Теперь перейдем к подробному описанию сервера STM 3104 с использованием фиг. 6. Сервер STM - это в действительности основной элемент области ветви подписки, и его задачей является управление бесплатными правами, подключение новых подписчиков и восстановление существующих подписчиков. Как показано на фиг. 6, команды передаются в генератор сообщений MG 3106, но в другом формате, отличном от того, в котором они передаются серверу STM. Сервер STM приспособлен для отправки сообщения подтверждения для каждой команды в CI только в том случае, когда соответствующая команда успешно обработана и отослана в MG.

Сервер STM содержит базу данных подписчиков 3120, в которой хранится вся информация о подписчиках (номер смарт-карты, коммерческие предложения, состояние, группа и положение в группе и т.д.). База данных выполняет семантические проверки команд, пересылаемых CI 3102, на соответствие содержимому базы данных и обновляет базу данных, когда команды являются допустимыми.

Сервер STM управляет также буфером типа FIFO 3122 между сервером STM и MG, а также резервным диском FIFO 3124. Назначение буферов FIFO состоит в усреднении потока команд от CI, если MG не в состоянии некоторое время ответить по какой-либо причине. Можно также гарантировать, что в случае аварийного отказа сервера STM или MG ни одна команда не будет потеряна, поскольку сервер STM выполняет очистку буферов FIFO (т.е., пересылку в MG) при перезапуске. Буферы FIFO реализованы в виде файлов.

Сервер STM содержит в своем ядре сервер автоматического восстановления 3126, который автоматически генерирует восстановления, и, при наличии запроса от оператора, бесплатные права. В этом смысле генерирование восстановления можно рассматривать как включающее генерирование прав для первого раза, хотя будет понятно, что генерирование новых прав инициируется в SMS. Как будет очевидно, обе эти команды могут обрабатываться как приблизительно одинаковые команды и EMM.

Размещение STM отдельно от SMS, и сервера автоматического восстановления - в SAS, а не в SMS 3004 (как в известных системах), является особенно важным отличием, поскольку это значительно уменьшает количество команд, которые необходимо передавать от SMS в SAS (учитывая то, что SMS и SAS могут располагаться в разных местах и ими могут управлять разные операторы). Фактически две основные команды, требуемые от SMS, - это команды запуска новой подписки и прекращения существующей подписки (например, в случае неплатежа). Путем минимизации обмена командами между SMS и SAS уменьшается возможность отказа при передаче команды по каналу 3006 между ними; кроме этого, проектирование SMS, вообще говоря, не требует учета особенностей системы условного доступа 3000.

Выполнение автоматического восстановления показано на блок-схеме, приведенной на фиг. 7. Для того, чтобы уменьшить требуемую пропускную способность, и в предположении, что в подавляющем количестве восстановления являются стандартными, восстановление производится по группам

подписчиков; в предпочтительных реализациях количество индивидуальных подписчиков в группе равно 256. Блок-схема начинается с начального шага 3130 и переходит к шагу 3132, где производится ежемесячное активирование функции восстановления (хотя, конечно, будет понятно, возможны и другие частоты восстановления). С частотой в один месяц конечному пользователю предоставляются права на текущий месяц и весь следующий месяц, после чего права исчерпываются, если они не восстановлены.

На шаге 3134 производится обращение к базе данных подписчиков по группам и по индивидуальным подписчикам в группе, чтобы определить, должны ли быть восстановлены права для конкретного индивидуально подписчика.

На шаге 3136 устанавливается битовый массив группы подписчиков в соответствии с содержимым базы данных подписчиков, как показано на фиг.8. Битовый массив содержит идентификатор группы ("G1" для группы 1) 3138 и 256 зон индивидуальных подписчиков 3140. Индивидуальные биты в битовом массиве устанавливаются равными 1 или 0, в зависимости от того, будут ли восстановлены права конкретного подписчика. На чертеже приведен типовой набор двоичных данных.

На шаге 3142 в генератор сообщений 3106 передаются соответствующие команды, включая битовый массив группы подписчиков. На шаге 3143 генератор сообщений устанавливает дату исчерпания прав, чтобы указать смарт-карте дату, по истечении которой EMM данной подписки становится недействительным;

обычно эта дата устанавливается равной концу следующего месяца. На шаге 3144 генератор сообщений генерирует на основе команд сообщения EMM для соответствующей группы подписчиков и требует от шифровального блока 3008 зашифровать сообщения EMM, а сообщения EMM будут затем отправлены инжектору EMM 3300, который на шаге 3146 вставляет эти сообщения в поток данных MPEG-2.

Шаг 3148 указывает, что описанная выше процедура повторяется для каждой группы. И, наконец, обработка завершается и прекращается на шаге останова 3150.

Описанная выше блок-схема, представленная на фиг.7, фактически относится специально к восстановлению подписки. Таким же образом STM управляет бесплатными зрительскими правами и новыми подписчиками.

В случае бесплатных зрительских прав, имеющих место для некоторых конкретных телевизионных программ или групп таких программ, они делаются доступными с помощью STM путем отправки генератору сообщений команды генерировать соответствующие зрительские EMM (для всех зрителей) с датой исчерпания прав, заданной количеством дней (или недель). MG вычисляет точную дату исчерпания прав на основе команды STM.

В случае появления новых подписчиков, они обрабатываются в два этапа. Сначала, при покупке смарт-карты для приемника/декодера 2020, по желанию оператора подписчику предоставляются бесплатные права на заданный период времени (обычно несколько дней). Это достигается путем генерирования для подписчика битового массива, который содержит соответствующую дату исчерпания прав. Затем подписчик передает полностью оформленные бумаги оператору, курирующему данного подписчика (в SMS). Как только бумаги обработаны, SMS передает в SAS команду запуска для конкретного подписчика. После приема SAS команды запуска, STM посылает в MG команду назначить новому подписчику уникальный адрес (с конкретным номером группы и позицией в группе) и сгенерировать специальное так называемое сообщение EMM подписки по "коммерческому предложению" (в противоположность обычному EMM групповой подписки, используемому для восстановления) для предоставления прав конкретному подписчику до конца следующего месяца. С этого момента восстановление подписчика может происходить автоматически, как описано выше. На этих двух этапах процесса можно предоставить новым подписчикам права до тех пор, пока SMS не выдаст команду останова.

Следует отметить, что EMM подписки на коммерческое предложение используется для новых подписчиков и для повторного активирования существующих подписчиков. EMM групповой подписки используется с целью восстановления и приостановки.

На фиг. 9 собственно типовое EMM подписки, представленное само по себе, (т. е. с игнорированием заголовка и подписи) с помощью упомянутой выше процедуры, состоит из следующих основных частей: как правило 256-битовый массив подписки (или группы подписчиков) 3152, 128 битов

шифровальных ключей управления 3154 для шифрования EMM, 64 бита для каждого шифровального ключа обработки 3156, чтобы позволить смарт-карте 3020 дешифровать слово управления с целью обеспечить доступ к программам вещания, и 16 битов даты истечения прав 3158 для указания даты, по истечении которой смарт-карта будет игнорировать EMM. Фактически в предпочтительной реализации предоставляются три ключа обработки, один устанавливается для текущего месяца, один устанавливается для следующего месяца и один для целей восстановления в случае отказа системы.

Более подробно, EMM групповой подписки должно содержать все эти компоненты, за исключением шифровальных ключей управления 3154. EMM подписки на коммерческое предложение (которое предназначено для индивидуального подписчика) должно содержать вместо битового массива всех подписчиков группы 3152 идентификатор группы ID, за которым следует позиция в группе, затем шифровальные ключи управления 3154 и три ключа обработки 3156, за которыми следует соответствующая дата истечения прав 3158.

Генератор сообщений MG 3106 служит для преобразования команд, выдаваемых сервером STM 3104, в EMM, для передачи в источник сообщения 3302. Как показано на фиг.5, сначала MG выдает собственно EMM и передает их в шифровальный блок CU 3008 для шифрования с использованием ключей управления и обработки. CU представляет EMM подпись 3064 (см. фиг.3) и передает EMM обратно в MG, где к нему добавляется заголовок. Сообщения EMM, которые передаются в источник сообщения, являются, таким образом, полными сообщениями EMM. Генератор сообщений также определяет время начала и окончания вещания и скорость выдачи сообщений EMM и пересылает эти данные в качестве указаний вместе с сообщениями EMM в источник сообщений. MG только один раз выполняет генерирование данного EMM, и именно ME выполняет их циклическую передачу.

Как показано на фиг.5, генератор сообщений содержит свою собственную базу данных EMM 3160, в которой EMM хранится в течение его жизненного цикла. Как только временной интервал выдачи сообщения заканчивается, оно уничтожается. База данных используется для того, чтобы обеспечить соответствие между MG и ME, так, чтобы, например, когда конечный пользователь не активен, ME не продолжал посылать восстановления. В подобной ситуации MG выполняет соответствующие операции и пересылает их в ME.

После генерирования EMM MG присваивает EMM уникальный идентификатор ID. Когда MG передает EMM в ME, он пересылает также EMM ID. Это обеспечивает идентификацию конкретного EMM как в MG, так и в ME.

Относительно области ветви подписки следует также отметить, что генератор сообщений содержит два FIFO 3162 и 3164, по одному для каждого из сообщений, относящихся к источникам сообщений 3302 и 3304 в инжекторе EMM 3300, для хранения шифрованных сообщений EMM. Поскольку область ветви подписки и инжектор EMM могут быть разнесены на значительное расстояние, использование FIFO может обеспечить полную непрерывность передачи EMM даже в случае отказа каналов 3166 и 3168 между ними. Два точно таких же FIFO имеются и в области ветви оплаты за просмотр (PPV).

Особенность, в частности, генератора сообщений и, в общем, системы условного доступа касается способа, с помощью которого уменьшается размер собственно EMM 3062 путем объединения параметра размера и идентификатора с целью экономии памяти. Это будет описано с помощью фиг. 10, на которой приведен в качестве примера EMM (это PPV-EMM, которое является простейшим EMM). Уменьшение размера происходит в идентификаторе Pid (сокращение от "packet identifier" или "parameter identifier") 3170. Он состоит из двух частей: самого идентификатора (ID) 3172 и параметра размера пакета 3174 (необходимого для того, чтобы идентифицировать начало следующего пакета). Весь Pid помещается точно в одном байте информации, 4 бита отводятся для ID и четыре бита для размера. Поскольку для определения размера с помощью двоичного числа четырех битов явно недостаточно, используется специальное соответствие между указанными битами и фактическим размером; это соответствие описывается справочной таблицей, хранящейся в области памяти 3178 генератора сообщений (см. фиг. 5). Обычно это следующее соответствие:

0000=0

0001=1

0010=2

0011=3

0100=4

0101=5

0110=6

0111=7

1000=8

1001=9

1010=10

1011=11

1100=12

1101=16

1110=24

1111=32

Как видно, параметр размера не является прямо пропорциональным фактическому размеру пакета - связь скорее квадратичная, чем линейная. Этим обеспечивается больший диапазон допустимых значений размера пакета.

#### Область ветви оплаты за просмотр (PPV)

Что касается области ветви оплаты за просмотр (PPV) 3200, подробно изображенной на фиг. 5, сервер санкционирования AS 3202 имеет в качестве своего клиента централизованный сервер заказов OCS 3207, который запрашивает информацию о каждом подписчике, который связывается с серверами связи 3022 с целью приобретения продукта PPV.

Если подписчик известен AS 3202, выполняется набор транзакций. Если подписчик санкционирован для заказа, AS формирует счет и посылает его в OCS. В противном случае она сигнализирует в OCS, что заказ не санкционирован.

Только по завершении всего этого набора транзакций AS обновляет базу данных конечных пользователей 3204 с помощью серверов (DBAS) 3206, если хотя бы одна транзакция санкционирована; таким образом оптимизируется количество обращений к базе данных.

Критерии, в соответствии с которыми AS санкционирует покупку, хранятся в базе данных, доступ к которой осуществляется с помощью DBAS. В одной из реализации база данных является той самой базой данных, которая доступна STM.

В зависимости от параметров пользователя санкционирование может быть отклонено (PPV\_Forbidden, Casino\_Forbidden,...). Такие критерии обновляются STM 3104 от имени SMS 3004.

Проверяются и другие параметры, такие как допустимые пределы для покупки (по кредитной карте, либо автоматическим платежам, либо по количеству покупок с отметкой санкционирования в день).

В случае платежа по кредитной карте проверяется наличие номера кредитной карты в локальном черном списке, хранящемся в базе данных локальных черных списков 3205.

Если все проверки успешны, AS:

1) формирует счет и пересылает его в OCS, которая завершает обработку этого счета и записывает его в файл; затем этот файл пересылается в SMS для обработки (фактическая выписка счета потребителю);

2) обновляет базу данных, в основном для установления новых пределов покупок.

Этот механизм "проверить-и-сгенерировать-счет-если-все-в-порядке" применяется для каждой команды, которую подписчик может запросить во время одиночного соединения (можно заказать, например, 5 фильмов за один сеанс).

Следует отметить, что AS имеет ограниченное количество информации о подписчике по сравнению с тем, которым обладает SMS. Например, AS не хранит имя и адрес подписчика. С другой стороны, AS имеет номер смарт-карты подписчика, потребительскую категорию подписчика (так что разным подписчикам могут быть сделаны разные предложения), и различные флаги, которые указывают, например, может ли подписчик выполнять покупки в кредит, или кредит приостановлен, или его смарт-карта похищена. Использование сокращенного объема информации может помочь уменьшить количество времени, затрачиваемое на санкционирование запроса конкретного подписчика.

Основной целью DBAS 3206 является увеличение производительности базы данных с точки зрения AS путем распараллеливания доступа (поэтому в действительности не имеет большого смысла создавать конфигурацию только с одной DBAS). AS определяет, сколько DBAS следует подключить. Данная DBAS может быть подключена только к одной AS.

OCS 2307 работает в основном с командами PPV. Она работает в нескольких режимах.

Во-первых, она обрабатывает команды, генерируемые SMS, такие как обновление продукта (например, если счет уже записан с помощью SMS, OCS счет не генерирует), обновление "кошелька" в смарт-карте 3020, и прекращение/возобновление сеанса.

Различными стадиями данной процедуры являются:

- 1) идентификация соответствующего подписчика (с использованием AS 3202);
- 2) если он действителен, формирование адекватных команд для генератора сообщений с целью отсылки соответствующего EMM. Команды могут быть:

Командами продукта,

Обновления "кошелька",

Уничтожения сеанса.

Следует отметить, что эти операции не предполагают выписки счетов, поскольку выписка счетов уже известна от SMS. Эти операции подобны покупке "бесплатного продукта".

Во-вторых, OCS обрабатывает команды, принимаемые от подписчиков через серверы связи 3022. Эти команды могут приниматься либо через модем, подключенный к приемнику/декодеру 2020, либо активироваться голосом через телефон 4001, либо активироваться клавишами с помощью MINITEL, PRESTEL или подобной системы там, где она имеется.

В-третьих, OCS имеет дело с запросами обратного вызова, выдаваемыми SMS. Эти последние два режима работы будут описаны подробнее ниже.

В описанном выше режиме второго типа OCS работает с командами, принимаемыми непосредственно от конечного пользователя (подписчика) через серверы связи CS 3022. К таким командам относятся запросы заказа продуктов (например, конкретной передачи PPV), команды изменения параметров подписки, и переопределения родительского кода (родительский код - это код, по которому родители могут ограничить детям право доступа к определенным программам или классам программ).

Способ, с помощью которого эти команды обрабатываются, ниже будет описан более подробно со ссылкой на фиг. 11.

Заказы подписчиками продукта включают следующие шаги:

- 1) идентификация с помощью AS абонента, который выполняет вызов через CS 3022, заказывая конкретный продукт;



- 2) проверка действительности запроса абонента опять-таки с использованием AS (куда запрос помещается с использованием приемника/декодера 2020, что достигается путем проверки данных смарт-карты 3020);
- 3) выяснение цены покупки;
- 4) проверка того, не превышает ли цена предела кредита абонента, и т.п.;
- 5) прием частичного счета от AS;
- 6) заполнение дополнительных полей в счете для формирования полного счета;
- 7) добавление полного счета в файл информации о счетах 3212 для последующей обработки;
- 8) отсылка соответствующей команды (или команд) в генератор сообщений PPV 3210 для генерирования соответствующего EMM (или нескольких EMM).

EMM (или несколько EMM) отсылается(ются) либо по модемному каналу 4002, если потребитель размещал заказ продукта с использованием приемника/декодера 2020 (более подробно это будет описано ниже), либо, в противном случае, передаются путем вещания. Единственное исключение имеет место тогда, когда в модемном канале происходит сбой (в случае, когда потребитель размещает заказ с использованием приемника/декодера); в этом случае EMM передается путем вещания через эфир.

Изменения параметров подписки, запрашиваемые подписчиком, включают:

- 1) идентификацию абонента (с использованием AS);
- 2) посылку информации в интерфейс команд CI; CI, в свою очередь переправляет эту информацию в SMS;
- 3) через CI OCS принимает затем ответ от SMS (в виде стоимости данного изменения, если таковое возможно).

Если изменение запрашивается с использованием приемника/декодера, OCS генерирует подтверждение для SMS. В противном случае, например, в случае вызова по телефону или через Minitel, подтверждение запрашивается у подписчика, и этот ответ отсылается в SMS через OCS и CI.

Переопределение родительского кода включает:

- 1) идентификацию абонента (с использованием AS);
- 2) посылку в MG команды генерирования соответствующего EMM, содержащего соответствующий пароль переопределения.

В случае переопределения родительского кода команда переопределения кода, из соображений безопасности, не может поступать от приемника/декодера. Такая команда может поступать только от SMS, через телефон или Minitel и т. п. Следовательно, в данном конкретном случае сообщения EMM только вещаются через эфир, и никогда не передаются по телефонной линии.

Из приведенных выше примеров различных режимов работы OCS понятно, что пользователь может иметь прямой доступ к SAS, и, в частности, OCS и AS, и что серверы связи подключаются непосредственно к SAS, и, в частности, к OCS. Эта важная особенность связана с уменьшением для пользователя времени передачи его команды в SAS.

Эта особенность иллюстрируется далее с помощью фиг. 12, из которой можно увидеть, как телеприставка конечного пользователя, и, в частности, приемник/декодер 2020, имеет возможность связываться непосредственно с серверами связи 3022, связанными с SAS 3002. Вместо осуществления связи между конечным пользователем и серверами связи 3022 системы SAS 3002 через SMS 3004, связь осуществляется непосредственно с SAS 3002.

Фактически обеспечиваются два прямых канала связи.



Первая прямая связь осуществляется по голосовому каналу через телефон 4001 и соответствующую телефонную линию (и/или через MINITEL или подобную связь, если имеется), когда конечные пользователи все еще должны вводить наборы голосовых команд или кодовых номеров, но по сравнению со связью через SMS 3004 время связи сокращается.

Вторая прямая связь осуществляется от приемника/декодера 2020, и ввод данных производится автоматически путем вставки конечным пользователем своей собственной дочерней смарт-карты 3020, в результате чего конечный пользователь освобождается от работы по вводу соответствующих данных, что, в свою очередь, уменьшает затрачиваемое время и вероятность ошибок во время ввода.

Следующая важная особенность, которая следует из сказанного выше, касается уменьшения времени, затрачиваемого на передачу сформированного EMM конечному пользователю для того, чтобы инициировать просмотр конечным пользователем выбранного продукта.

Вообще говоря, в соответствии с фиг.12, эта особенность достигается, опять-таки, за счет предоставления приемнику/декодеру 2020 конечного пользователя возможности прямой связи с серверами связи 3022, связанными с SAS 3002.

Как описано выше, совмещенный приемник/декодер 2020 непосредственно подключается к серверам связи 3022 через модемный обратный канал 4002, так что команды от декодера 2020 обрабатываются SAS 3002, генерируются сообщения (включая EMM) и затем отсылаются обратно в декодер 2020 по обратному каналу 4002. Для связи между CS 3022 и приемником/декодером 2020 используется протокол (как будет описано ниже), так что CS принимает подтверждение приема соответствующего EMM, таким образом повышая надежность процедуры.

Тогда, например, в случае режима предварительного заказа SAS 3002 принимает сообщения от конечного пользователя через смарт-карту и декодер 2020, через модем и через телефонную линию 4002, запрашивающие доступ к конкретной передаче/продукту, и возвращает соответствующее EMM по телефонной линии 4002 и модем в декодер 2020, причем предпочтительно, чтобы модем и декодер были бы размещены вместе в оконечной пользовательской приставке (STB - Set-Top-Box). Таким образом конечному пользователю обеспечивается возможность просмотра передачи/продукта без необходимости передачи EMM в потоке данных MPEG-2 2002 через мультимплексор и скремблер 2004, канал "земля-спутник" 2012, спутник 2014 и канал "спутник-земля" 2016. Это в существенной степени уменьшает время и требуемую пропускную способность. Обеспечивается наверняка, что как только подписчик заплатит за покупку, в приемник/декодер 2020 приходит EMM.

В режиме работы описанной выше OCS 3207 третьего типа, OCS имеет дело с запросами обратных вызовов, выдаваемых SAS. Это проиллюстрировано на фиг.13. Цель типовых запросов обратного вызова - обеспечение того, что приемник/декодер 2020 выполняет обратный вызов SAS через обратный модемный канал 4002, направляя информацию, которая требуется SAS от приемника/декодера.

В соответствии с инструкциями интерфейса команд 3102 генератор сообщений ветви подписки генерирует и отправляет в приемник/декодер 2020 EMM обратного вызова. Из соображений безопасности это EMM зашифровывается с помощью блока шифрования 3008. EMM может содержать время/дату, когда приемник/декодер должен "проснуться" и выполнить свой собственный обратный вызов, без прямого запрашивания; EMM обычно может также содержать номера телефонов, которые терминал должен набрать, количество последующих попыток после неудачных вызовов, и задержку между двумя вызовами.

После приема EMM или достижения заданных времени/даты приемник/декодер 2020 связывается с серверами связи 3022. OCS 3207 сначала идентифицирует абонента с помощью AS 3202 и проверяет определенные данные, такие как о владельце смарт-карты и подписчике. Затем OCS запрашивает смарт-карту 3020 переслать различную зашифрованную информацию (такую как соответствующие номера сеансов, когда сеанс просматривался, сколько раз подписчику разрешено повторно просматривать сеанс, режим просмотра сеанса, количество оставшихся жетонов, количество предварительно заказанных сеансов и т.д.). Эта информация расшифровывается генератором сообщений ветви PPV 3210, опять-таки с использованием шифровального блока 3008. OCS добавляет эту информацию в файл информации обратного вызова 3214 для дальнейшей обработки и передачи в SMS 3004. Из соображений безопасности эта информация зашифровывается. Вся процедура повторяется до тех пор, пока со смарт-карты не будет считано вся доступная информация.

Особенно предпочтительной особенностью средства обратного вызова является то, что перед

чением смарт-карты (сразу же после идентификации абонента с использованием AS 3202, как описано выше) с помощью SAS 3002 выполняется проверка того, что приемник/декодер действительно является подлинным, а не пиратской версией или компьютерной имитацией. Эта проверка производится следующим образом. SAS генерирует случайное число, которое принимается приемником/декодером, зашифровывается и затем возвращается в SAS. SAS дешифрует это число. Если дешифровка прошла успешно и извлечено исходное случайное число, делается вывод, что приемник/декодер является подлинным, и процедура продолжается. В противном случае процедура прерывается.

Другими функциями, которые могут выполняться при обратном вызове, являются стирание устаревших сеансов со смарт-карты или пополнение кошелька (это будет описано ниже в разделе "Смарт-карта").

В отношении области ветви оплаты за просмотр (PPV) 3200, ниже приведено описание серверов связи CS 3022. На уровне аппаратного обеспечения, в предпочтительном варианте реализации, они представляют собой машину DEC с четырьмя процессорами. На уровне архитектуры программного обеспечения, показанной на фиг. 14, во многих отношениях серверы связи CS являются обычными. Одно важное отличие от традиционных конфигураций следует из того факта, что серверы должны обслуживать как приемник/декодер 2020, так и голосовую связь через обычные телефоны 4001, а также, возможно, MINTEL или аналогичные системы.

Следует между тем отметить, что на фиг.14 показаны два централизованных сервера заказов 3207 (OCS1 и OCS2). Конечно, может использоваться любое требуемое количество OCS.

К серверам связи относятся два главных сервера ("CS1" и "CS2"), а также некоторое число фронтальных серверов ("Frontal 1" и "Frontal 2"); хотя на чертеже показаны только два фронтальных сервера, обычно их 10 или 12 на каждый главный сервер. Действительно, хотя показаны два главных сервера, CS1 и CS2, и два фронтальных сервера, Frontal 1 и Frontal 2, может использоваться любое их количество. Обычно желательна некоторая избыточность.

CS1 и CS2 соединены с OCS1 и OCS2 через каналы TCP/IP 3230 верхнего уровня, тогда как CS1 и CS2 соединены с Frontal 1 и Frontal 2 через дополнительные каналы TCP/IP 3232.

Как показано, CS1 и CS2 содержат серверы для "SENDER" (передача), "RECEIVER" (прием), "VTX" (MINTEL, PRESTEL или им подобные), "VOX" (голосовая связь) и "TRM" (связь через приемник/декодер). Они подключены к шине "BUS" для обмена сигналами с фронтальными серверами.

CS1 и CS2 связываются непосредственно с приемниками/декодерами 2020 через их модемные обратные каналы 4002, используя открытый сетевой протокол X25. Между серверами связи 3022 и приемниками/декодерами 2020 используется протокол относительно низкого уровня, в одной предпочтительной реализации основанный на стандартном международном CCITT протоколе V42, который обеспечивает надежность благодаря наличию средств обнаружения ошибок и повторной передачи данных, а также использует подпрограмму проверки контрольных сумм для проверки целостности повторной передачи. Предусматривается также механизм прерывания для того, чтобы воспрепятствовать передаче недопустимых символов.

С другой стороны, голосовая телефонная связь осуществляется через фронтальные серверы связи, каждый из которых в состоянии одновременно обслуживать до, положим, 30 голосовых соединений от соединения 3234 с локальной телефонной сетью через высокоскоростные "T2" (E1) стандартные телефонные ISDN линии.

Тремя особыми функциями программной части серверов связи (которые в альтернативном варианте, конечно, могут быть полностью реализованы аппаратно) являются, во-первых, преобразование информации протокола относительно низкого уровня, принимаемой от приемника/декодера, в информацию протокола относительно высокого уровня, выводимую в OCS; во-вторых, распределение или управление количеством одновременно осуществляемых соединений; и в-третьих, обеспечение нескольких параллельных каналов без возникновения помех. Что касается последней функции, серверы связи играют в некотором роде роль мультиплексора при взаимодействии с конкретным каналом, определяемым ID (идентификатором) сеанса, который фактически используется во всей цепочке связи.

В завершение того, что касается области ветви оплаты за просмотр (PPV) 3200, показанной на фиг. сервер для вещания программ (SPB) 3208 подключен к одному или нескольким вещателям программ РВ 3250 (которые обычно являются удаленными от SAS) для приема информации программы. SPB отфильтровывает для дальнейшего использования информацию, соответствующую передачам PPV (сеансы).

Особенно важной особенностью является то, что отфильтрованная информация передачи программы передается SPB в MG, который, в свою очередь, посылает директиву (команду управления) в ME для изменения по обстоятельствам частоты циклической выдачи EMM; для выполнения этого ME отыскивает все EMM с идентификатором соответствующего сеанса и изменяет циклическую частоту, установленную для таких EMM. Эта особенность может рассматриваться как динамическое выделение полосы пропускания для конкретных EMM. Циклическая выдача EMM описывается более подробно в следующем ниже разделе, касающемся инжектора EMM.

Ниже будут описаны обстоятельства, при которых производится изменение циклической частоты, со ссылкой на фиг. 15, которая демонстрирует, как циклическая частота 3252 повышается за короткое время (скажем, 10 минут) перед передачей определенной программы PPV и до конца программы, от низкой циклической частоты, скажем, один раз каждые 30 минут, до высокой циклической частоты, скажем, один раз каждые 0,5-1 минуту, для того, чтобы удовлетворить в это время ожидаемые дополнительные запросы от пользователей на передачи PPV. Таким способом полоса пропускания может выделяться динамически, в соответствии с прогнозируемыми запросами пользователя. Это может помочь уменьшить требования к пропускной способности.

Циклическая частота других EMM также может варьироваться. Например, циклическая частота EMM подписки может варьироваться путем посылки мультиплексором и скремблером 2004 соответствующих директив о скорости обмена.

#### Инжектор EMM

Что касается инжектора EMM 3300, источники сообщений 3302-3308, являющиеся частью инжектора EMM и функционирующие в качестве средства вывода для генератора сообщений, подробно описываются с помощью фиг. 16. Их функция состоит в получении сообщений EMM и их циклической передаче (по типу карусели) через соответствующие каналы 3314 и 3316 в программные мультиплексоры 3310 и 3312 и далее в аппаратные мультиплексоры и скремблеры 2004. В ответ мультиплексоры и скремблеры 2004 генерируют глобальную директиву скорости передачи для управления всеми циклическими частотами сообщений EMM; для этого ME принимают во внимание различные параметры, такие как время цикла, размер EMM и т.д. На чертеже EMM\_X и EMM\_Y - это группы EMM для операторов X и Y, в то время, как EMM-Z представляют собой другие EMM, для оператора X либо Y.

Далее рассмотрим подробно один из источников сообщений ME; отметим, что остальные ME функционируют точно таким же образом. ME работает под управлением директив от MG, основные из которых - время начала и окончания трансляции и частота выдачи, а также номер сеанса, если EMM представляет собой EMM PPV. Что касается частоты выдачи, в предпочтительной реализации соответствующая директива может принимать одно из пяти значений - от Very fast (очень часто) до Very slow (очень редко). В директиве не указываются численные значения, но вместо этого ME отображает директиву на фактическое числовое значение, которое предоставляется соответствующей частью SAS. В предпочтительном варианте реализации имеется пять следующих частот выдачи:

1. Very fast (очень часто) - каждые 30 секунд.
2. Fast (часто) - каждую минуту.
3. Medium (умеренно) - каждые 15 минут.
4. Slow (редко) - каждые 30 минут.
5. Very slow (очень редко) - каждые 30 минут.

ME имеет первую и вторую базу данных 3320 и 3322. Первая база данных предназначена для тех EMM, дата вещания которых еще не наступила; они хранятся в базе данных последовательно в

файлах, упорядоченных по времени. Вторая база данных предназначена для EMM, подлежащих немедленному вещанию. На случай аварийного отказа системы МЕ организованы таким образом, чтобы иметь возможность повторного считывания соответствующего записанного файла и выполнения правильного вещания. Все хранящиеся в базе данных файлы обновляются по запросу от MG, которое обеспечивает соответствие между поступающими директивами и уже отосланными в МЕ EMM. Вещаемые EMM также хранятся в оперативной памяти 3324.

Использование FIFO 3162 и 3164 в генераторе сообщений в комбинации с базами данных 3320 и в источнике сообщений обеспечивает функционирование их обоих в автономном режиме, если канал 3166 между ними окажется временно поврежден; МЕ все еще сможет осуществлять вещание EMM.

Программные мультиплексоры (SMUX) 3310 и 3312 обеспечивают интерфейс между МЕ и аппаратными мультиплексорами 2004. В предпочтительной реализации все они принимают EMM от двух МЕ, хотя в общем случае ограничений на количество МЕ, которые могут быть подключены к одному SMUX, не существует. Мультиплексоры SMUX накапливают EMM и затем пересылают их согласно типу EMM в соответствующие аппаратные мультиплексоры. Это необходимо потому, что аппаратные мультиплексоры принимают сообщения EMM разных типов и помещают их в разные места потока MPEG-2. Кроме этого, SMUX направляют глобальные директивы скорости передачи от аппаратных мультиплексоров в МЕ.

Очень важная особенность МЕ состоит в том, что он выдает EMM в случайном порядке. Причина состоит в следующем. Источник сообщений не имеет возможности определять или контролировать то, что он передает в мультиплексор. Следовательно, возможно, что он может передать два EMM, которые должны быть приняты и декодированы в приемнике/декодере 2020, непосредственно одно за другим. При таких обстоятельствах в ситуации, когда EMM недостаточно разделены, возможно, что приемник/декодер и смарт-карта будут не в состоянии надлежащим образом воспринять и декодировать второе EMM. Циклическая передача EMM в случайном порядке может разрешить эту проблему.

Ниже с использованием фиг. 17 будет описан способ, с помощью которого достигается рандомизация; в предпочтительной реализации необходимая программная логика реализуется с помощью компьютерного языка ADA. Особенно важной частью рандомизации является правильное хранение EMM в базах данных 3320 и 3322 (которые используются с целью резервирования) и в оперативной памяти 3324. Для конкретной циклической частоты и оператора EMM сохраняют в двумерных массивах, по классам 3330 (скажем, в порядке от А до Z), и по номерам в классах 3332 (от 0 до N). Добавляется третье измерение, соответствующее циклической частоте 3334, так что получается, что число двумерных массивов равно количеству циклических частот. В предпочтительном варианте реализации имеется 256 классов, и в каждом классе - от 200 до 300 сообщений EMM; имеется пять циклических частот. Последнее измерение добавляется к массиву наличием разных операторов; имеется столько трехмерных массивов, сколько операторов. Хранение данных в таком виде может обеспечить быстрый поиск в случае, когда MG желает удалить конкретное EMM.

Хранение сообщений EMM осуществляется согласно алгоритму хеширования (известному еще "односторонняя функция хеширования"). Оно выполняется на основе функции остатка от деления, так что сначала классы заполняются поочередно, и затем начинают использоваться старшие номера классов, при этом количество EMM в каждом классе остается приблизительно постоянным. В рассмотренном здесь примере 256 классов. Когда MG посылает в МЕ EMM с идентификатором (ID) 1, этому EMM присваивается класс "1", и оно занимает первый номер 3332 в классе 3330. EMM с ID 2 присваивается класс "2", и так далее до класса 256. EMM с ID 257 опять присваивается класс "1" (на основе функции остатка от деления), и он занимает второй номер в первом классе, и т.д.

Поиск конкретного EMM, например, когда MG запрашивает удаление конкретного EMM, осуществляется с помощью процедуры, обратной по отношению к описанной выше. Алгоритм хеширования применяется к ID EMM для определения класса, после чего устанавливается номер класса.

Фактическая рандомизация происходит тогда, когда сообщения EMM циклически извлекаются из оперативной памяти 3324 с использованием средств рандомизации 3340, которые реализуются в аппаратном и/или программном обеспечении источника сообщений. Извлечение осуществляется случайным образом и, опять-таки, основано на алгоритме хеширования. Во-первых, выбирается случайное число (для приведенного выше примера - в диапазоне от 1 до 256), чтобы определить необходимый класс. Во-вторых, выбирается еще одно случайное число, чтобы определить

необходимый номер в классе. Это второе случайное число выбирается с учетом общего числа EMM в данном классе. Как только данное EMM выбрано и его вещание выполнено, оно перемещается во вторую идентичную область памяти в ПЗУ 3324, опять-таки с использованием функции хеширования. Таким образом, по мере вещания сообщений EMM первая область уменьшается в размере, и, как только будет использован весь класс, он удаляется. Как только первая область памяти полностью опустошается, перед новым циклом вещания EMM она заменяется второй областью памяти, и наоборот.

После двух или трех циклов вещания EMM описанным выше способом шансы того, что любые два EMM, предназначенные для одного конечного пользователя будут переданы непосредственно одно за другим, с точки зрения статистики, пренебрежимо малы.

Через равные интервалы, пока производится сохранение сообщений EMM, компьютер 3050 вычисляет количество байтов памяти и на основе этого вычисляет скорость передачи для выдачи сообщений с учетом глобальной директивы скорости передачи от мультиплексора и программного мультиплексора.

Выше были упомянуты резервные базы данных 3320 и 3322. В предпочтительной реализации они представляют собой последовательные файлы, в которых хранится резервная версия содержимого оперативной памяти 3324. В случае отказа источника сообщений и последующего перезапуска или, в более общем случае, когда ME перезапускается по какой-либо причине, между оперативной памятью и базами данных формируется канал, по которому записанные EMM загружаются в оперативную память. Таким способом может быть устранен риск потери сообщений EMM в случае отказа.

Точно так же, как описано выше, происходит запись EMM PPV для EMM подписки, причем класс обычно соответствует данному оператору, и номер в классе соответствует номеру сеанса.

#### Смарт-карта

Дочерняя смарт-карта, или смарт-карта подписчика, схематически изображена на фиг. 18 и содержит 8-битовый микропроцессор 110, такой как микропроцессор Motorola 6805, имеющий шину ввода/вывода, подключенную к стандартному массиву контактов 120, которые при использовании подключаются к соответствующему массиву контактов устройства считывания смарт-карты приемника/декодера 2020, имеющего обычную конфигурацию. Микропроцессор 110 соединен посредством шины с предпочтительно маскированным ПЗУ 130, ОЗУ 140 и электрически-стираемым программируемым ПЗУ 150. Смарт-карта соответствует стандартам ISO 7816-1, ISO 7816-2 и ISO 7816-3, которые определяют некоторые физические параметры смарт-карты, позиции контактов микросхемы и некоторые связи между внешней системой (и, в частности, приемником/декодером 2020) и смарт-картой соответственно, и поэтому далее описываться не будет. Одной из функций микропроцессора 110 является управление памятью смарт-карты, как описано ниже.

Электрически-стираемое программируемое ПЗУ 150 содержит динамически создаваемые разделы операторов 154, 155, 156 и динамически создаваемые разделы данных, которые будут описаны ниже с использованием фиг. 19.

Как показано на фиг. 19, электрически-стираемое программируемое ПЗУ 150 содержит постоянный раздел ID смарт-карты (или производителя) 151 из 8 битов, который содержит постоянный идентификатор смарт-карты подписчика, установленный производителем смарт-карты 3020.

При установке смарт-карты микропроцессор 110 выдает сигнал приемнику/декодеру 2020, который содержит идентификатор системы условного доступа, используемый смарт-картой, и данные, формируемые на основе данных, хранящихся в смарт-карте, включая ID смарт-карты. Этот сигнал сохраняется приемником/декодером 2020, который затем использует записанный сигнал для проверки совместимости смарт-карты с системой условного доступа, используемой приемником/декодером 2020.

Электрически-стираемое программируемое ПЗУ 150 содержит также постоянный раздел генератора случайных чисел 152, который содержит программу для генерирования псевдослучайных чисел. Эти случайные числа используются для диверсификации сигналов выходных транзакций, генерируемых смарт-картой 3020 и пересылаемых обратно в устройство вещания.

Ниже раздела генератора случайных чисел 152 представлен постоянный раздел управления 153

размером 144 байта. Постоянный раздел управления 153 - это специальный раздел оператора, используемый программой в ПЗУ 130 при динамическом создании (и удалении) разделов 154, 155, 156, как будет описано ниже. Постоянный раздел управления 153 содержит данные, относящиеся к правам смарт-карты по созданию и удалению разделов.

Программа динамического создания и удаления разделов вызывается в ответ на специальные ЕММ создания (или удаления) конкретного раздела, которые передаются SAS 3002, принимаются приемником/декодером 2020 и передаются в смарт-карту 3020 подписчика. Для создания таких ЕММ оператору необходимы специальные коды-ключи для раздела управления. Это не позволяет оператору удалять разделы, относящиеся к другому оператору.

Ниже раздела управления 153 находится последовательность разделов "ID оператора" 154, 155, 156 для операторов 1, 2N соответственно. Как правило по крайней мере один раздел идентификатора оператора предварительно загружается в электрически-стираемое программируемое ПЗУ смарт-карты подписчика 3020, так что конечный пользователь может дешифровать программы, вещаемые этим оператором. Последующие разделы идентификаторов оператора могут позже создаваться динамически с использованием раздела управления 153 в ответ на сигнал выходной транзакции, формируемый конечным пользователем (подписчиком) с помощью его смарт-карты 3020, как будет описано далее.

Каждый раздел оператора 154, 155, 156 содержит идентификатор группы, к которой принадлежит смарт-карта 3020, и позицию смарт-карты в группе. Эти данные позволяют смарт-карте (вместе с другими смарт-картами этой группы) отвечать на вещание ЕММ групповой подписки, имеющий адрес этой группы (но не позицию смарт-карты в группе), а также на индивидуальные ЕММ (подписки на коммерческие предложения), адресованные только данной смарт-карте группы. В каждой группе может быть до 256 смарт-карт-членов, и эта особенность значительно уменьшает требуемую пропускную способность, необходимую для вещания ЕММ.

Для того, чтобы еще более уменьшить требуемую пропускную способность, необходимую для вещания ЕММ групповой подписки, данные группы в каждом разделе оператора 154, 155, 156 и всех подобных разделах в электрически -стираемом программируемом ПЗУ смарт-карты 3020 и других дочерних смарт-карт непрерывно обновляются, чтобы позволить конкретной смарт-карте изменить свое положение в каждой группе, заполняя таким образом "дыры", создаваемые, например, в результате удаления карты-члена группы. Дыры заполняются SAS 3002, поскольку список этих дыр находится в сервере STM 3104.

Таким образом уменьшается фрагментация, и количество членов в каждой группе поддерживается примерно равным максимальному числу 256 членов.

Каждый раздел оператора 154, 155, 156 связан с одним или несколькими "объектами данных оператора", хранящимися в электрически-стираемом программируемом ПЗУ 150. Как показано на фиг. 19, последовательность динамически создаваемых объектов данных оператора 157-165 располагается ниже разделов идентификаторов оператора. Каждый из этих объектов помечается с помощью:

- а) идентификатора 1, 2, 3N, соответствующего связанному с ним оператору 1, 2, 3N, как показано в левой части фиг. 19;
- б) ID, указывающего тип объекта; и
- с) раздела данных, зарезервированного для данных, как показано в правой части каждого соответствующего объекта данных оператора на фиг. 19. Следует понимать, что каждому оператору соответствует набор объектов данных, подобный наборам объектов данных иных операторов, так что описание типов данных в объекте данных оператора 1 применимо также для объектов данных всех других операторов. Кроме этого, следует отметить, что объекты данных располагаются в физически смежных областях электрически-стираемого программируемого ПЗУ, и что порядок их следования несущественен.

Удаление объекта данных создает "дыру" 166 в смарт-карте, т.е. количество байтов, которые ранее занимал удаленный объект, не занимают немедленно. "Освободившееся" таким образом количество байтов, или "дыра", помечаются:

- а) идентификатором оператора 0; и



б) ID, указывающим, что байты свободны для приема объекта.

Следующий создаваемый объект данных заполняет дыру, идентифицируемую идентификатором 0. Таким образом обеспечивается эффективное использование ограниченного объема памяти (4 килобайта) электрически-стираемого программируемого ПЗУ 150.

Обращаясь к набору объектов данных, соответствующих каждому оператору, ниже будут описаны примеры таких объектов данных.

Объект данных 157 содержит ключ ЕММ, используемый для дешифровки зашифрованных ЕММ, принимаемых приемником/декодером 2020. Это ключ ЕММ постоянно хранится в объекте данных 157. Этот объект данных 157 может быть создан заранее, до продажи смарт-карты 3020, и/или может быть создан динамически при создании нового раздела оператора (как описано выше).

Объект данных 159 содержит ключ ЕСМ, который пересылается соответствующим оператором (в данном случае, оператором 1), чтобы позволить конечному пользователю дешифровать конкретный "букет" программ, на которые он подписался. Обычно новые ключи ЕСМ рассылаются каждый месяц вместе с ЕММ групповой подписки (восстановления), которое восстанавливает все права конечного пользователя на просмотр вещания от оператора (в данном случае - оператора 1). Использование отдельных ключей ЕММ и ЕСМ позволяет продавать права на просмотр разными способами (в данной реализации - по подписке и индивидуально (оплата за просмотр - PPV)) и также улучшает защиту. Режим оплаты за просмотр (PPV) будет описан ниже.

Поскольку периодически посылаются новые ключи ЕСМ, важно не допустить использование пользователем старых ключей ЕСМ, например, путем выключения приемника/декодера или переустановки часов, с целью предупредить истечение срока действительности старого ключа ЕСМ, перекрывая таймер приемника/декодера 2020. В соответствии с этим раздел оператора 154 содержит область (обычно имеющую размер 2 байта), содержащую дату истечения срока действительности ключей ЕСМ. Смарт-карта 3020 имеет возможность сравнить эту дату с текущей датой, которая содержится в принятых ЕСМ, и воспрепятствовать дешифровке, если текущая дата превышает дату истечения срока действительности ключей ЕСМ. Дата истечения срока действительности передается с помощью сообщений ЕММ, как описано выше.

Объект данных 161 содержит 64-битовый массив подписки, который является точным представлением программ оператора вещания, на которые подписался подписчик. Каждый бит соответствует одной программе и устанавливается в "1", если подписка на программу оформлена, и в "0", если нет.

Объект данных 163 содержит некоторое количество жетонов, которые могут быть использованы клиентом в режиме PPV для приобретения прав просмотра приближающегося вещания, например, в ответ на бесплатный анонс или какое-либо другое объявление. Объект данных 163 содержит также предельное значение, которое может быть задано, например, отрицательным, что делает возможным кредитование клиента. Жетоны могут быть приобретены, например, в кредит с помощью обратного модемного канала 4002, или, например, с использованием голосового сервера в сочетании с кредитной карточкой. За каждую передачу может взиматься плата как в один жетон, так и в несколько.

Объект данных 165 содержит описание PPV-передачи, как показано в справочной табл. 167 на фиг.20.

Структура 167, описывающая PPV-передачи, содержит поля "ID сеанса" 168, идентифицирующее сеанс просмотра (соответствующий программе, а также времени и дате вещания), "режим сеанса" 169, указывающий, как приобретено право просмотра (например, в режиме предварительного заказа), "индекс сеанса" 170 и "просмотр сеанса" 171.

При приеме программы в режиме PPV приемник/декодер 2020 определяет, является ли программа продаваемой в режиме PPV. Если это так, декодер 2020 проверяет, с использованием данных, хранящихся в структуре 167, описывающей PPV-передачу, сохранено ли в ней поле "ID сеанса" данной программы. Если поле "ID сеанса" там сохранено, то слово управления извлекается из ЕСМ.

Если поле "ID сеанса" там не сохранено, то с помощью специального приложения приемник/декодер 2020 выдает конечному пользователю сообщение, указывающее, что он имеет право просмотра

данного сеанса по цене, скажем, 25 жетонов, как считано из ECM, или должен связаться с сервером связи 3022, чтобы купить программу. При использовании жетонов, если конечный пользователь отвечает "да" (с помощью удаленного контроллера 2026 (см. фиг. 2)), декодер 2020 посылает ECM в смарт-карту, смарт-карта уменьшает кошелек смарт-карты 3020 на 25 жетонов, сохраняет поля "ID сеанса" 168, "режим сеанса" 169, "индекс сеанса" 170 и "просмотр сеанса" 171 в структуру описания PPV-передачи 167 и извлекает из ECM и дешифрует слово управления.

В режиме предварительного заказа EMM будет передано в смарт-карту 3020, так что смарт-карта сохранит поля "ID сеанса" 168, "режим сеанса" 169, "индекс сеанса" 170 и "просмотр сеанса" 171 в структуре 167 описания PPV-передачи с использованием EMM.

Поле "индекс сеанса" 170 предусмотрено для различения вещательных трансляций друг от друга. Это средство позволяет осуществлять санкционирование для подмножества вещательных трансляций, например, для 3 из 5 трансляций. Как только ECM с индексом сеанса, отличным от текущего значения поля "индекса сеанса" 170, хранящегося в структуре 167 описания PPV-передачи, передается в смарт-карту, значение поля "просмотр сеанса" 171 уменьшается на единицу. Когда значение поля "просмотр сеанса" достигнет нуля, смарт-карта откажется дешифровать ECM с индексом сеанса, отличным от текущего поля "индекс сеанса".

Исходное значение поля "просмотр сеанса" зависит только от способа, которым оператор вещания желает определить передачу, к которой оно относится; поля "просмотр сеанса" для каждой программы может принимать любое значение.

В микропроцессоре 110 смарт-карты реализована программа подсчета и сравнения для обнаружения такого момента, когда исчерпан лимит на количество просмотров какой-либо программы.

Указанные поля "ID сеанса" 168, "режим сеанса" 169, "индекс сеанса" 170 и "просмотр сеанса" 171 структуры 167 описания PPV-передачи могут быть извлечены из смарт-карты с помощью процедуры "обратного вызова", как было описано выше.

Каждый приемник/декодер 2020 содержит идентификатор, который может идентифицировать приемник/декодер уникальным образом, или может классифицировать его тем или иным способом для того, чтобы позволить ему работать только с конкретной индивидуальной смарт-картой, конкретным классом смарт-карт одного и того же, либо соответствующего, производителя, или любым другим классом смарт-карт, который предназначен для использования исключительно с этим классом приемников/декодеров.

Таким образом, приемник/декодер 2020, который был поставлен потребителю одним из операторов вещания, защищается от использования несанкционированных дочерних смарт-карт 3020.

Дополнительно или в качестве альтернативы к этому первому квитированию связи между смарт-картами и приемником, электрически стираемое программируемое ПЗУ смарт-карты 3020 может содержать поле или битовый массив, описывающий категории приемников/декодеров 2020, с которыми она может работать. Они могут задаваться либо во время изготовления смарт-карты, либо с помощью специального EMM.

Битовый массив, хранящийся в смарт-карте 3020, обычно содержит список, включающий до 80 приемников/декодеров, каждый из которых идентифицируется соответствующим ID приемника/декодера, с которым смарт-карта может использоваться. В соответствие каждому приемнику/декодеру ставится значение "1" или "0", указывающее, соответственно, может или нет смарт-карта использоваться с данным приемником/декодером. Программа в памяти 2024 приемника/декодера отыскивает идентификатор этого приемника/декодера в битовом массиве, хранящемся в смарт-карте. Если идентификатор найден, и соответствующее идентификатору значение равно "1", смарт-карта "разрешается"; если нет, смарт-карта не будет работать с этим приемником/декодером.

Дополнительно, если обычно вследствие соглашения между операторами желательно санкционировать использование в конкретном приемнике/декодере других смарт-карт, "первым" смарт-картам будут посланы через ретранслятор 2014 специальные EMM с целью изменения их битовых массивов.

Каждый оператор вещания может дифференцировать своих подписчиков в соответствии с заранее



определенными критериями. Например, некоторое число подписчиков может быть классифицировано как "VIP" (очень важные лица). Соответственно, каждый оператор вещания может разделить своих подписчиков на множество подмножеств, каждое подмножество может состоять из любого числа подписчиков.

Подмножество, к которому принадлежит конкретный подписчик, устанавливается в SMS 3004. В свою очередь, SAS 3002 передает подписчику EMM, которое записывает информацию (обычно длиной 1 байт) о подмножестве, к которому подписчик принадлежит, в соответствующий раздел данных оператора, скажем, 154, электрически-стираемого программируемого ПЗУ смарт-карты. В свою очередь, по мере того, как оператор вещания осуществляет вещание программ, вместе с программой передается ЕСМ, обычно из 256 битов, указывающее, какое подмножество подписчиков может просматривать программу. Если, согласно информации, хранящейся в разделе оператора, подписчик не имеет права на просмотр передачи, что определяется ЕСМ, просмотр программы запрещается.

Это средство может использоваться, например, для выключения всех смарт-карт данного оператора в конкретном географическом регионе во время трансляции конкретной программы, в частности, программы, связанной со спортивным мероприятием, проводимым в данном географическом регионе. Таким способом футбольные клубы и другие спортивные организации могут продавать права трансляции за пределами их локального региона, одновременно запрещая локальным болельщикам просмотр мероприятия по телевизору. Таким образом болельщики локального региона стимулируются к приобретению билетов и посещению мероприятия.

Каждая из особенностей, связанная с разделами от 151 до 172, рассматривается как отдельное изобретение, независимо от того, создается ли раздел динамически.

Очевидно, что настоящее изобретение было описано выше исключительно в виде примера, и возможны различные модификации в пределах данного изобретения.

Каждая особенность, изложенная в описании, а также (где это уместно) пункты формулы и чертежи могут быть предоставлены независимо или в соответствующем сочетании.

В вышеупомянутых предпочтительных вариантах реализации некоторые средства предлагаемого изобретения реализованы с использованием программного обеспечения. Однако опытному специалисту, конечно, понятно, что любые эти средства могут быть реализованы аппаратно. Далее, понятно, что функции, выполняемые аппаратными средствами, программное обеспечение компьютера и тому подобное выполняются на или с использованием электрических и им подобных сигналов.

Перекрестные ссылки выполнены на наши совместно рассматриваемые заявки с той же самой датой подачи и озаглавленные как "Генерирование сигналов и вещание" (номер дела поверенного PC/ASD/19707), "Смарт-карта для использования в приемнике зашифрованных вещательных сигналов и приемник" (номер дела поверенного PC/ASD/19708), "Система вещания и приема и система условного доступа для нее" (номер дела поверенного PC/ASD/19710), "Загрузка компьютерного файла из передатчика через приемник/декодер в компьютер" (номер дела поверенного PC/ASD/19711), "Трансляция и прием телевизионных программ и других данных" (номер дела поверенного PC/ASD/19712), "Загрузка данных" (номер дела поверенного PC/ASD/19713), "Организация памяти компьютера" (номер дела поверенного PC/ASD/19714), "Разработка системы управления телевидением и радио" (номер дела поверенного PC/ASD/19715), "Извлечение разделов данных из потока транслируемых данных" (номер дела поверенного PC/ASD/19716), "Система управления доступом" (номер дела поверенного PC/ASD/19717), "Система обработки данных" (номер дела поверенного PC/ASD/19718), "Система вещания и приема, а также приемник/декодер и удаленный контроллер для нее" (номер дела поверенного PC/ASD/19720). Раскрытие содержимого этих документов включено сюда посредством ссылок. Список заявок включает и предлагаемое изобретение.

### ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система условного доступа для системы вещания и приема, отличающаяся тем, что она содержит: средство генерирования множества сообщений, предназначенных для предоставления конечному пользователю прав на доступ к одной или более передачам, выдаваемым передатчиком упомянутой системы вещания и приема; приемник/декодер для приема упомянутых передач и упомянутых сообщений с целью предоставления конечному пользователю доступа к одной или более из указанных передач, а также для передачи в упомянутое средство генерирования сообщений данных

запроса на осуществление упомянутого доступа, и сервер связи, подключенный непосредственно к упомянутому средству генерирования сообщений, причем упомянутое средство генерирования сообщений выполнено с возможностью генерирования сообщения, предназначенного для предоставления прав, в ответ на данные запроса, передаваемые в средство генерирования сообщений от упомянутого приемника/декодера через упомянутый сервер связи, и с возможностью осуществления связи с упомянутым приемником/декодером через упомянутый сервер связи для передачи приемнику/декодеру упомянутого сообщения, предназначенного для предоставления прав.

2. Система условного доступа по п. 1, дополнительно содержащая спутниковый ретранслятор, в которой упомянутое средство генерирования сообщений выполнено с возможностью передачи сообщения, предназначенного для предоставления прав, в виде пакета цифровых данных на упомянутый приемник/декодер либо через упомянутый сервер связи, либо через упомянутый спутниковый ретранслятор.

3. Система условного доступа по п. 1 или 2, в которой упомянутый приемник/декодер выполнен подключаемым к упомянутому серверу связи через модем и телефонный канал.

4. Система вещания и приема, включающая систему условного доступа по любому из предшествующих пунктов.

5. Система вещания и приема по п. 4, в которой упомянутый сервер связи выполнен с возможностью осуществлять специализированную связь между приемником/декодером и средством генерирования сообщений.

6. Система вещания и приема по п. 5, дополнительно содержащая модем, причем упомянутое средство генерирования сообщений подключено к упомянутому модему через упомянутый сервер связи.

7. Система вещания и приема по любому из пп. 4-6, в которой упомянутый приемник/декодер содержит средство для чтения смарт-карты, вставляемой в него конечным пользователем, которая содержит сохраненные данные для автоматического инициирования передачи сообщения от упомянутого приемника/декодера в упомянутое средство генерирования сообщений после вставки смарт-карты конечным пользователем.

8. Система вещания и приема по любому из пп. 4-7, содержащая дополнительно голосовой канал обеспечения связи со средством генерирования сообщений конечному пользователю системы вещания и приема.

9. Система вещания и приема по любому из пп. 4-8, в которой упомянутый приемник/декодер содержит средство для приема сжатых сигналов MPEG-типа, средство декодирования принятых сигналов для получения телевизионного сигнала и средство подачи телевизионного сигнала в телевизор.

10. Система условного доступа для системы вещания и приема, предназначенная для обеспечения условного доступа для подписчиков, отличающаяся тем, что она содержит: систему управления подписчиками для хранения данных, касающихся подписки на упомянутую систему вещания и приема; систему санкционирования подписчиков, подключенную к системе управления подписчиками для использования данных, принимаемых от упомянутой системы управления подписчиками, при формировании сообщений, предназначенных для предоставления прав на доступ к одной или более передачам, выдаваемым передатчиком упомянутой системы вещания и приема; и сервер связи, подключенный непосредственно к системе санкционирования подписчиков; причем упомянутая система санкционирования подписчиков выполнена с возможностью генерирования сообщения, предназначенного для предоставления прав, в ответ на данные запроса на упомянутый доступ, принимаемые через упомянутый сервер связи.

11. Система условного доступа по п. 10, дополнительно содержащая приемник/декодер для подписчика, причем упомянутый приемник/декодер выполнен так, что возможно его подключение к упомянутому серверу связи и тем самым к упомянутой системе санкционирования подписчиков через модем и телефонный канал.

12. Система условного доступа по п. 11, дополнительно содержащая спутниковый ретранслятор, причем упомянутая система санкционирования подписчиков выполнена с возможностью передачи

сообщения, предназначенного для предоставления прав, в виде пакета цифровых данных на упомянутый приемник/декодер либо через сервер связи, либо через спутниковый ретранслятор.

13. Система условного доступа по п. 11 или 12, в которой упомянутый приемник/декодер выполнен так, что возможно его подключение к упомянутому серверу связи через модем и телефонный канал.

14. Система условного доступа по любому из пп. 11-13, в которой сообщения, предназначенные для предоставления прав, генерируются системой санкционирования подписчиков в ответ на команду от приемника/декодера.

15. Система условного доступа для обеспечения доступа подписчика к одной или более передачам, выдаваемым передатчиком системы вещания и приема, с использованием приемника/декодера, содержащая сервер связи, выполненный с возможностью подключения к приемнику/декодеру подписчика, отличающаяся тем, что она также содержит: систему управления подписчиками для хранения информации о подписке; и систему санкционирования подписчиков для генерирования сообщений, предназначенных для предоставления прав на доступ, в ответ на команды, принимаемые через сервер связи, содержащую: централизованный сервер заказов, подключенный к серверу связи для приема команд от приемника/декодера и информации от системы управления подписчиками; сервер санкционирования, подключенный к централизованному серверу заказов для идентификации и проверки подписчика в ответ на запрос санкционирования от централизованного сервера заказов; и генератор сообщений, подключенный к централизованному серверу заказов, для генерирования сообщений, предназначенных для предоставления прав на доступ, в ответ на команду, принятую от централизованного сервера заказов; причем упомянутый централизованный сервер заказов выполнен с возможностью выдачи упомянутой команды в генератор сообщений в ответ на данные об идентификации и проверке подписчика, принимаемые от упомянутого сервера санкционирования, и/или данные о подписке, принимаемые от упомянутой системы управления подписчиками, и с возможностью передачи упомянутых сообщений, предназначенных для предоставления прав на доступ, в приемник/декодер через сервер связи.

16. Система вещания и приема, содержащая со стороны вещания систему вещания, включающую в себя средство для вещания запроса обратного вызова; и со стороны приема приемник, включающий в себя средство для осуществления обратного вызова системы вещания в ответ на запрос обратного вызова, отличающаяся тем, что она выполнена с возможностью проверки того, что упомянутый приемник является подлинным, с помощью упомянутого запроса обратного вызова.

17. Система вещания и приема по п. 16, в которой система вещания содержит средство для генерирования контрольного сообщения и передачи его в приемник, приемник содержит средство для шифрования контрольного сообщения и передачи его в систему вещания, и система вещания дополнительно содержит средство для дешифрования контрольного сообщения, принимаемого от приемника, и сравнения его с оригинальным контрольным сообщением.

18. Система по п. 16 или 17, в которой средство вещания выполнено с возможностью вещания запроса обратного вызова, который включает в себя команду, согласно которой обратный вызов осуществляется в заданное время, и средство для осуществления обратного вызова системы вещания выполнено с возможностью ответа на упомянутую команду.

19. Система вещания и приема, содержащая со стороны вещания: систему вещания, включающую в себя средство для вещания запроса обратного вызова; и со стороны приема: приемник, включающий в себя средство для осуществления обратного вызова системы вещания в ответ на запрос обратного вызова, отличающаяся тем, что запрос обратного вызова содержит команду, согласно которой обратный вызов осуществляется в заданное время, и средство для осуществления обратного вызова системы вещания выполнено с возможностью ответа на упомянутую команду.

20. Система по любому из пп. 16-19, в которой средство для осуществления обратного вызова системы вещания содержит модем, подключаемый к телефонной сети.

21. Система по любому из пп. 16-20, в которой средство для осуществления обратного вызова системы вещания выполнено с возможностью передачи в систему вещания информации о приемнике.

22. Система по п. 21, в которой система вещания содержит средство для хранения упомянутой информации.

23. Система по любому из пп. 16-22, в которой средство вещания выполнено с возможностью вещания в качестве запроса обратного вызова по меньшей мере одного сообщения, предназначенного для предоставления прав.

24. Система по любому из пп. 16-23, в которой запрос обратного вызова включает в себя команду, указывающую заданное количество попыток и интервалы между попытками обратного вызова.

25. Система по любому из пп. 16-24, в которой запрос обратного вызова включает команду, указывающую по меньшей мере один заданный телефонный номер, который должен быть набран средством для осуществления обратного вызова при ответе на запрос обратного вызова.

#### **РИСУНКИ**

Рисунок 1, Рисунок 2, Рисунок 3, Рисунок 4, Рисунок 5, Рисунок 6, Рисунок 7, Рисунок 8, Рисунок 9, Рисунок 10, Рисунок 11, Рисунок 12, Рисунок 13, Рисунок 14, Рисунок 15, Рисунок 16, Рисунок 17, Рисунок 18, Рисунок 19, Рисунок 20